



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/905,533

07/14/2001

Myles Jordan

062891.6294

3486

5073

7590

03/03/2006

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER

SCHUBERT, KEVIN R

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 03/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/905,533

Applicant(s)

JORDAN, MYLES

Examiner

Kevin Schubert

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 December 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claims 1-18 have been considered. Examiner maintains the rejections presented in the previous action. Additionally, a new 112, second paragraph, rejection has been which has been necessitated by Applicant's amendment.

5

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

10

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 17-18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims do not relate to matter residing in a tangible embodiment.

15

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

20

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1,2,7-12, and 17-18 recite the limitation "the viral detection alarm" (e.g. claim 1, lines 14-15). There is insufficient antecedent basis for this limitation in the claim. Claims 3-6 and 13-16 are also rejected based on their dependence on claims 1,2,7-12, and 17-18.

25

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

30

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said

Art Unit: 2137

subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5 Claims 1-4,6-14, and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg, U.S. Patent No. 6,357,008, in view of Trcka, U.S. Patent No. 6,453,345.

As per claims 1-2,7-12, and 17-18, the applicant describes a method for detecting decryption of encrypted viral code comprising the following limitations which are met by Nachenberg and Trcka:

- 10 a) emulating computer executable code in a subject file (Nachenberg: Col 7, lines 9-12);
- b) maintaining a list of memory regions that have been read and then modified during emulation (Nachenberg: Col 9, lines 5-10);
- c) flagging a memory area that is read during emulation of a first instruction in the computer executable code (Nachenberg: Col 9, lines 5-10);
- 15 d) detecting a modification to the flagged memory area during emulation of a second instruction in the computer executable code (Nachenberg: Col 9, lines 5-10);
- e) updating the list of memory regions to include the modified flagged memory area (Nachenberg: Col 9, lines 11-14);
- f) determining that one of the listed memory regions is larger than a predetermined size
- 20 (Nachenberg: Col 8, lines 1-30);
- f) triggering a viral detection in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code (Nachenberg: Col 8, lines 1-30; Trcka: Col 17, lines 24-34);

 Nachenberg discloses all the limitations of the above claim except for part f. With regard to part f,

25 Nachenberg discloses that if a memory region is not larger than a predetermined size it is regarded as non-viral and a first particular course of action is followed (e.g. directly entering the exploration phase). If a memory region is larger than a predetermined size, a second course of action is followed. However, Nachenberg does not disclose a viral detection alarm.

Art Unit: 2137

Trcka discloses the idea of a viral detection alarm. The use of an alarm serves many benefits, including alerting a user so that a user is informed and may take appropriate action. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Trcka with those of Nachenberg and use an alarm because doing so alerts a user so that he is informed of the
5 situation and may take appropriate action.

As per claims 3 and 13, the applicant discloses the method of claims 2 and 12, which are met by Nachenberg in view of Trcka, with the following limitation which is met by Nachenberg:

Wherein the emulation is performed on an instruction-by-instruction basis (Nachenberg: Col 7,
10 lines 55-67).

As per claims 4,6,14, and 16, the applicant discloses the method of claims 2 and 12, which are met by Nachenberg in view of Trcka, with the following limitation which is met by Nachenberg:

a) determining whether a selected one of the listed memory regions overlaps the modified
15 memory area (Nachenberg: Figure 4B);

b) updating the selected memory region to encompass the modified memory area (Nachenberg:
Col 9, lines 11-14).

Claims 5 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nachenberg,
20 U.S. Patent No. 6,357,008, in view of Trcka in further view of Nachenberg, U.S. Patent No. 6,971,019.

As per claims 5 and 15, the applicant discloses the method of claims 2 and 12, which are met by Nachenberg in view of Trcka, with the following limitation which is anticipated by Nachenberg:

a) determining whether a selected one of the listed memory regions is contiguous with the
25 modified memory area (Nachenberg: Figure 4B);

b) updating the selected memory region to encompass the modified memory area (Nachenberg:
Col 9, lines 11-14).

Art Unit: 2137

Regarding part a, Nachenberg (#6,357,008) in view of Trcka discloses comparing a selected one of the listed memory regions with the modified memory area but does not specifically disclose a determination that the regions are contiguous. Nachenberg (#6,971,019) discloses the well-known idea of determining a continuous memory area. It would have been obvious to one of ordinary skill in the art to combine the ideas of Nachenberg (#6,971,019) with those of Nachenberg (#6,357,008) in view of Trcka because doing so provides a further means to monitor for viral code.

Response to Arguments

Applicant has traversed Examiner's official notice of dependent claims 5 and 15 and has requested that Examiner find a reference. Accordingly, and in compliance with MPEP 2144.03, Examiner has supplied a reference for claims 5 and 15 in the instant action.

Applicant's arguments, see Remarks filed 2/7/06, with respect to the 103(a) rejection of claim 1 under Nachenberg in view of Trcka have been fully considered but they are not persuasive. Applicant presents the following argument:

(1) Nachenburg does not disclose parts f) and g) of instant claim 1

(2) Trcka does not disclose parts f) and g) of instant claim 1

Based on the above, Applicant believes the claimed invention is patentable. Such an argument is not persuasive on any level. To begin with, Examiner respectfully submits that the subject matter of parts f) and g) (substantially part f of previous action) was rejected **under the combination of Nachenburg and Trcka**. Examiner never indicated that the subject matter currently argued was taken individually from Nachenburg or individually from Trcka. Accordingly, an argument that Nachenburg and Trcka do not meet the subject matter by themselves, even if true, is moot.

In the instant case, Nachenburg discloses "determining that one of the listed memory regions is larger than a predetermined size" (part f). Further, Nachenburg teaches that if a memory region is larger than a predetermined size, a viral exploration course phase is followed. The Trcka reference has been

Art Unit: 2137

combined to teach a "viral alarm". Examiner has submitted that a "viral alarm" is well-known in the art and would have been an obvious combination into the system for at least the reason that doing so alerts a user so that he is informed of a situation and may take appropriate action.

Applicant argues that Nachenburg "would trigger an alarm after detecting suspicious behavior, but not in response to the size of a memory region" (Remarks, page 2). To what extent this statement is true, the rejection is not based on Nachenburg generating any type of alarm. The use of an alarm was taken from Trcka. Thus, such an argument does not overcome the rejection. Applicant also notes that Trcka fails to teach "determining that one of the listed memory regions is larger than a predetermined size" (Remarks, page 2). Even if true, Trcka has been incorporated merely for its teaching of a "viral alarm". Thus, such an argument does not overcome the rejection.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.


Art Unit: 2137

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application
5 Information Retrieval (PAIR) system. Status information for published applications may be obtained from
either Private PAIR or Public PAIR. Status information for unpublished applications is available through
Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should
you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC)
at 866-217-9197 (toll-free).

10

KS


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

15